**Network Monitoring and SIEM Tools**

**16.1. Network Monitoring**

Network monitoring is the process of continuously observing a computer network for any failures, performance issues, or abnormal behavior to ensure smooth operations and security. It involves tracking devices such as routers, switches, servers, firewalls, and endpoints using specialized tools.

Tools used to monitor the health, performance, and availability of network devices and services in real-time.

Purpose of Network Monitoring

* Ensure availability and uptime of network services.
* Detect and respond to failures or bottlenecks.
* Monitor bandwidth usage and traffic patterns.
* Maintain security by identifying unusual activities.
* Help in capacity planning and network optimization.

**16.2. Steps in Network Monitoring**

**16.2.1.  Network Mapping and Inventory**

* Identify all devices and components in the network.
* Create a network topology diagram.
* Inventory IP addresses, hostnames, MAC addresses, etc.

**16.2.2. Choose the Right Monitoring Tool**

* Select a tool that fits your network size and needs (e.g., Nagios, Zabbix, PRTG, SolarWinds).
* Make sure the tool supports necessary protocols like SNMP, ICMP, or WMI.

**16.2.3. Define Monitoring Parameters**

* Set what to monitor: CPU usage, memory, disk space, bandwidth, uptime, packet loss, etc.
* Specify thresholds for alerts.

**16.2.4. Configure Alerting and Notifications**

* Set up email, SMS, or Slack alerts for specific events.
* Define severity levels (Info, Warning, Critical).

**16.2.5. Implement Dashboards and Reports**

* Create real-time dashboards to visualize network health.
* Schedule reports for uptime, usage, and incidents.

**16.2.6 Monitor Traffic and Logs**

* Use tools to track real-time network traffic.
* Analyze logs for anomalies or policy violations.

**16.2.7. Analyze and Respond**

* Investigate alerts and take corrective actions.
* Identify root causes using historical data.

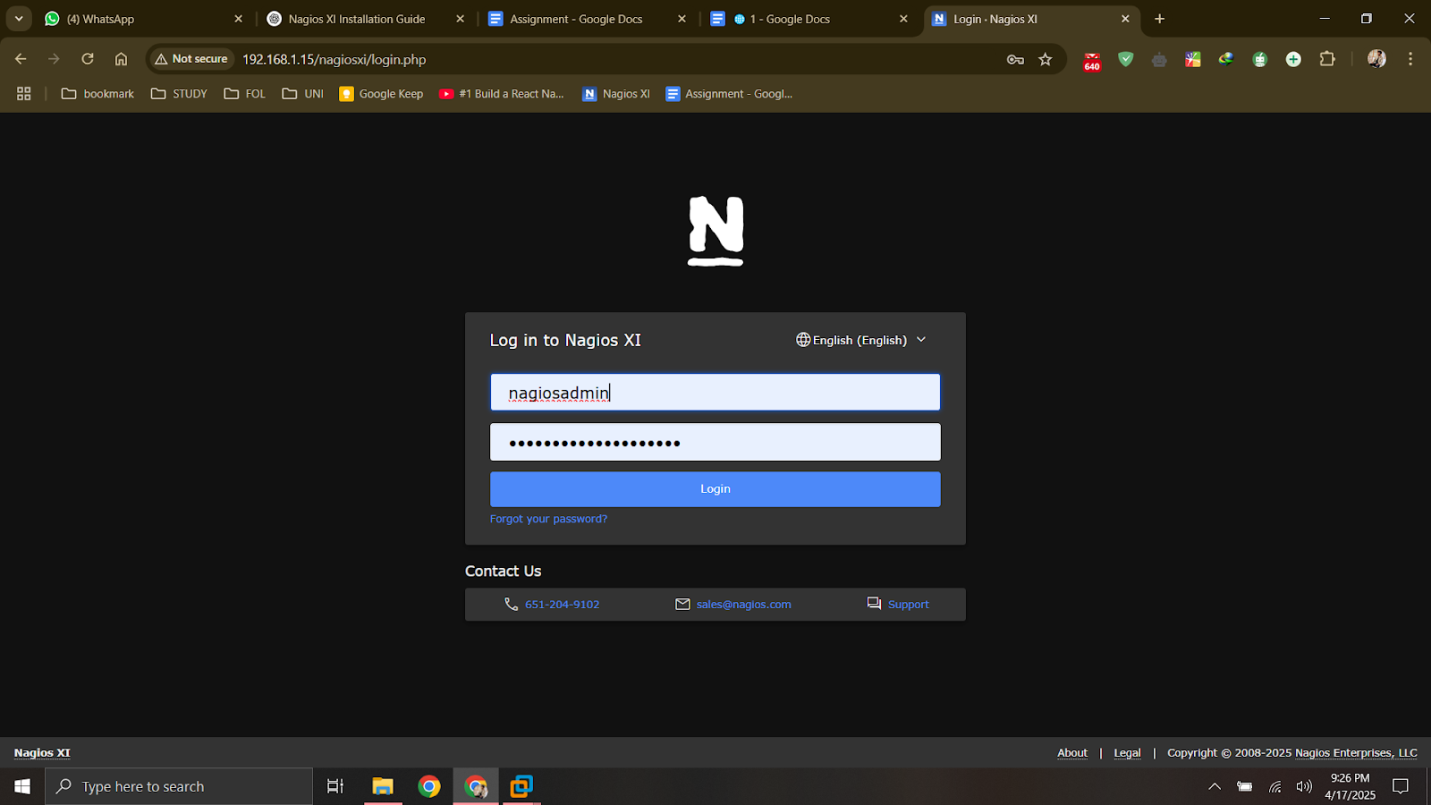
**16.2.8. Review and Optimize**

* Periodically review performance and modify thresholds.
* Upgrade tools or infrastructure as needed.

**16.3 Real time monitoring using Nagios XI**

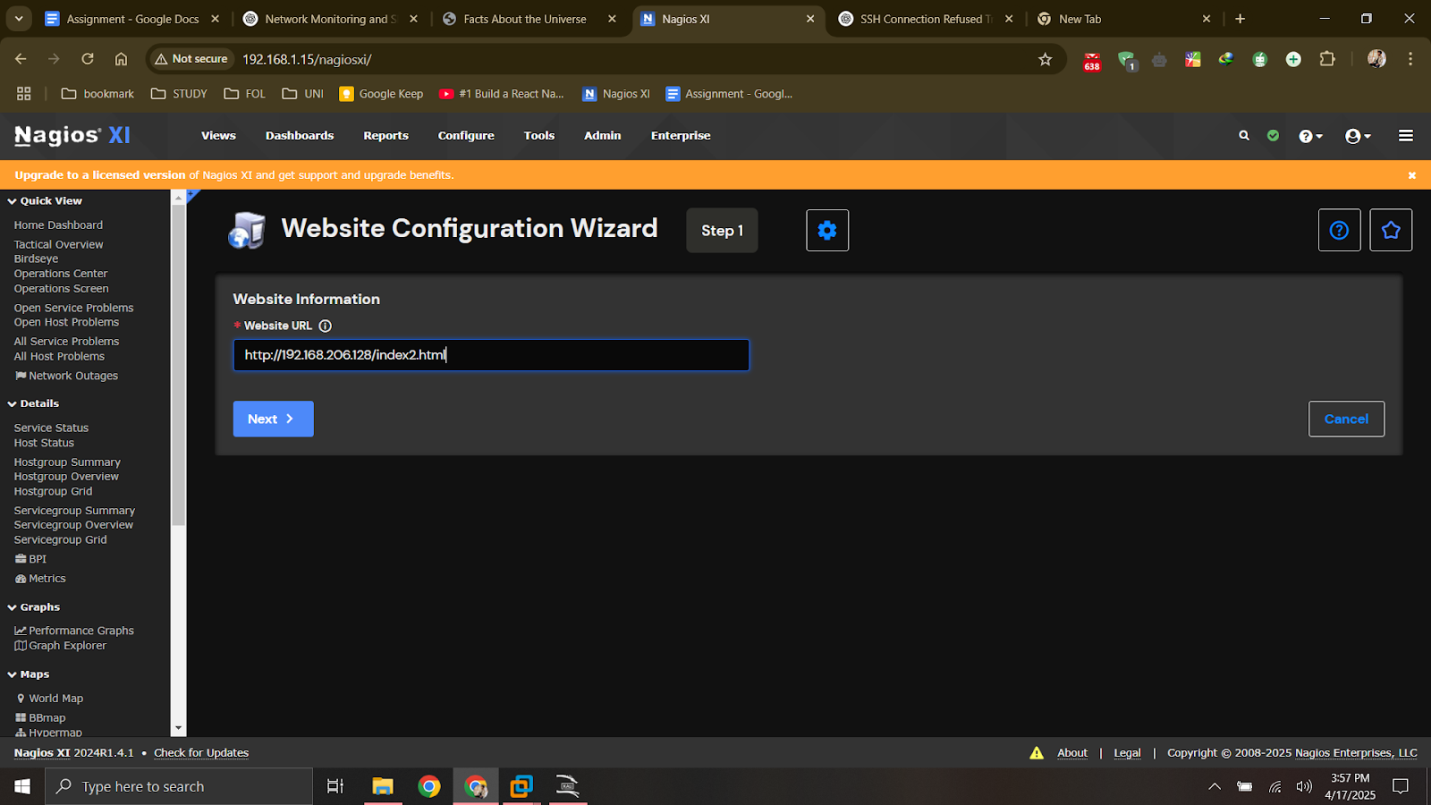
**16.3.1. Log into Nagios XI**

* Open your browser.
* Go to http://<your-nagios-server-ip>/nagiosxi
* Log in with your admin credentials.



**16.3.2. Use the Website Monitoring Wizard**

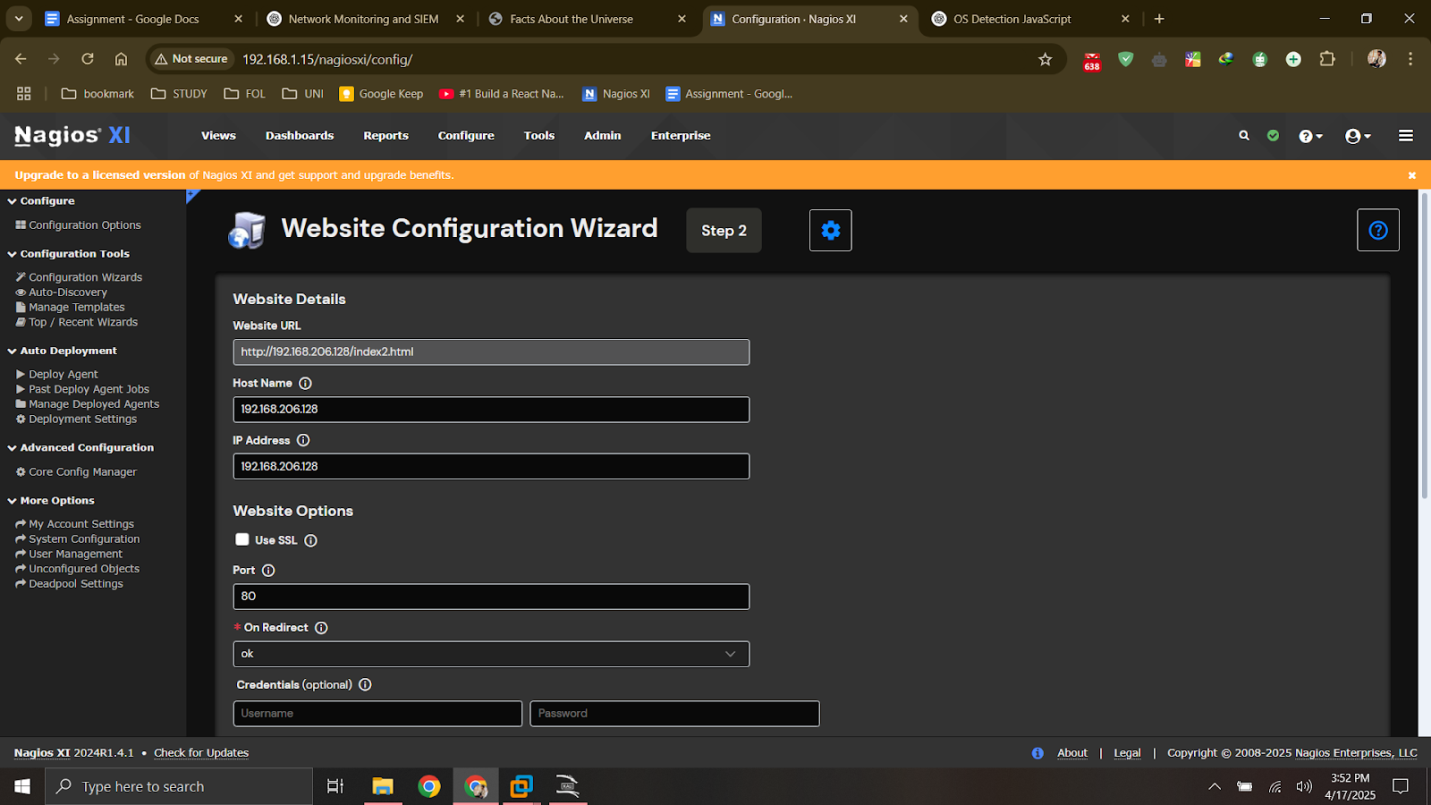
* Go to Configure → Configuration Wizards
* Select Website or Website URL wizard

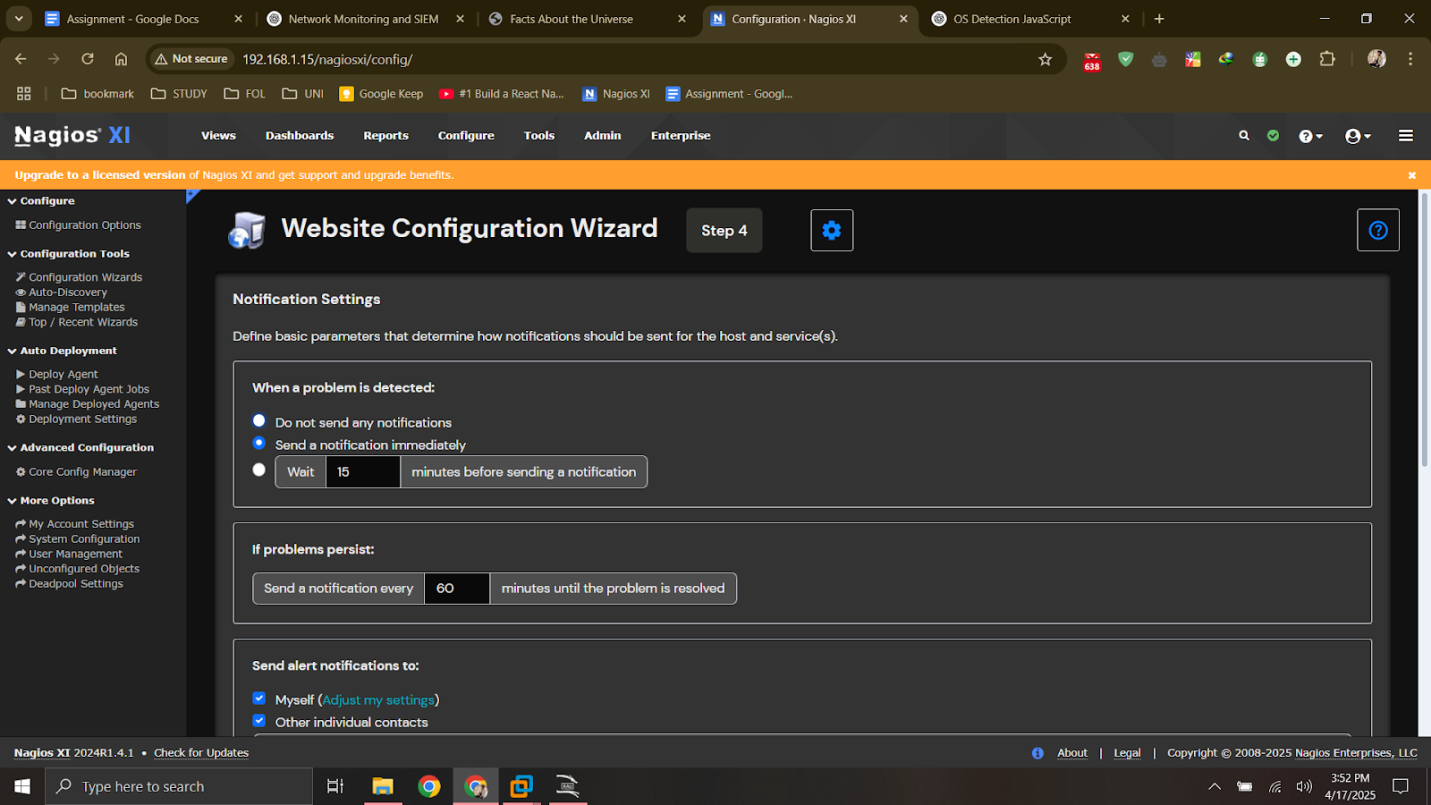


**16.3.3. Fill in Website Details**

You’ll be prompted to enter the following:

* URL to monitor: e.g., https://example.
* Host Name: A name for the host (e.g., ExampleSite)
* Max Check Attempts: Usually 5
* Check Interval: e.g., 5 minutes
* Retry Interval: e.g., 1 minute

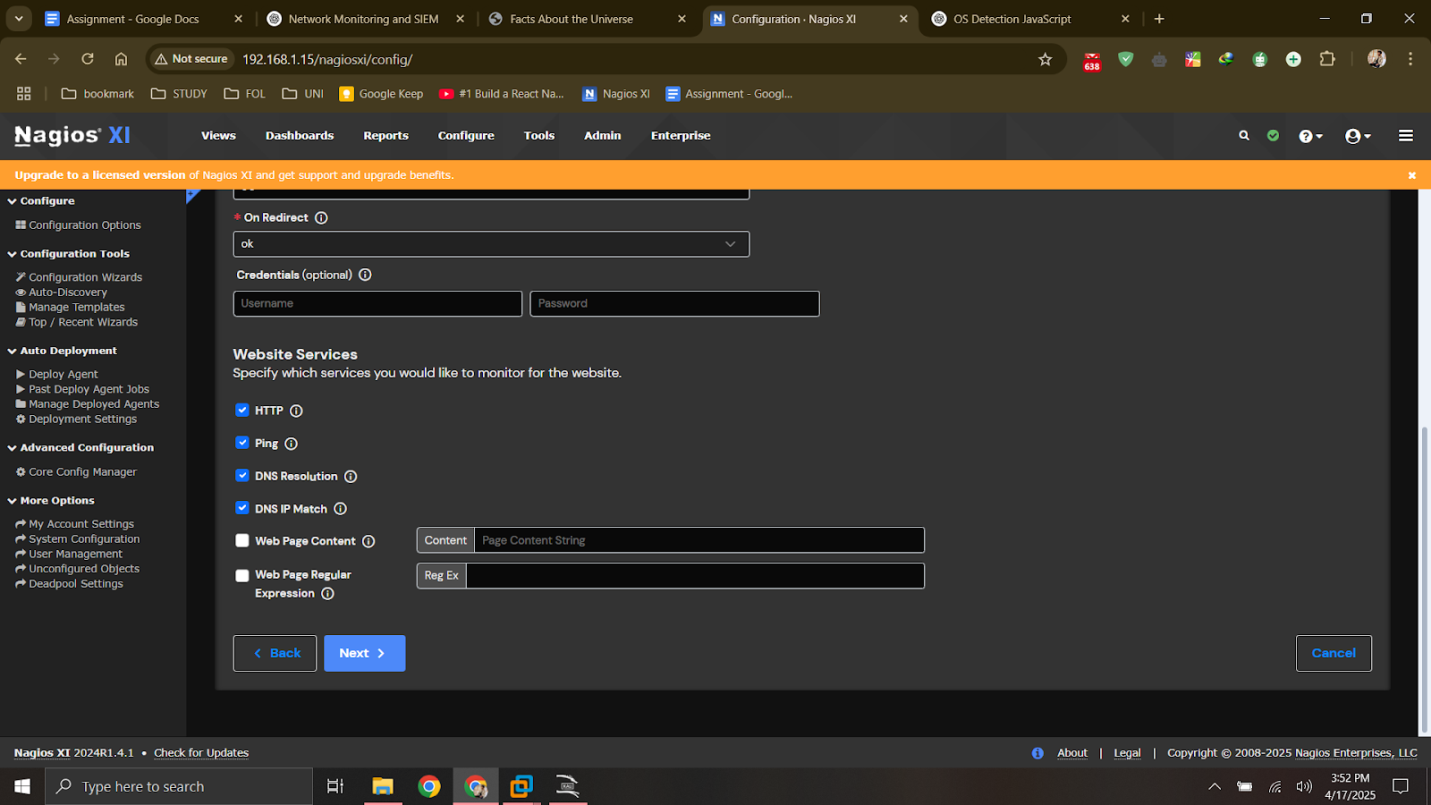




**16.3.4. Configure Advanced Checks (Optional)**

You can also set:

* Content match: Check if specific text (e.g., “index2”) is on the page.
* SSL certificate validity: To get alerts if the SSL cert is near expiry.
* Redirects & timeouts: Handle HTTP redirects or check response time.
* Authentication: If your site requires login (basic auth).



**16.3.5. Set Notifications**

* Choose contacts or contact groups to receive alerts if:
  + Site goes DOWN
  + Page content is missing
  + Response time is too slow

**16.3.6. Review & Apply Configuration**

* Click Next through the wizard
* Finish and Apply Configuration when prompted

**16.3.7. View Website Status**

* Go to Home → Host Services

